

ISTITUTO “F. SEVERI” - PADOVA
POLICY E REGOLAMENTO PER L’UTILIZZO DELLA RETE INFORMATICA

1. Premessa

All’interno del nostro Istituto sono operative tre distinte e fisicamente separate reti informatiche:

- A. Rete uffici, utilizzata per scopi amministrativi, riservata esclusivamente al personale amministrativo, anche in accesso remoto via VPN (smart working).
- B. Rete didattica ovvero rete laboratori, connessa ad Internet, collega tra loro tutti i laboratori, l’auditorium, la biblioteca e la sala docenti. Viene utilizzata:
 - i. con funzionalità tipiche della rete LAN per condividere risorse didattiche logiche e fisiche sia all’interno dei singoli laboratori che tra laboratori differenti tramite l’accesso al server del dominio;
 - ii. come punto di accesso a Internet per consentire a allievi ed insegnanti l’accesso al registro elettronico e la ricerca di materiali necessari allo svolgimento dell’attività didattica.
- C. Rete Wi-Fi, connessa ad Internet per consentire a allievi delle classi digitali e a tutti gli insegnanti l’accesso al registro elettronico e la ricerca di materiali necessari allo svolgimento dell’attività didattica.

2. Analisi dei rischi

L’Istituto segue le norme G.D.P.R. 679/16 art.37, par.7

Le reti didattica e Wi-Fi non contengono al proprio interno dati personali sensibili, ma sono comunque soggette a rischi, i principali dei quali sono legati a:

- A. utilizzo improprio delle risorse;
- B. accesso a siti non idonei all’ambiente scolastico;
- C. possibili attacchi provenienti da codice maligno (virus, worm, cavalli di Troia e simili);
- D. mancato rispetto della legislazione sul diritto d’autore.

Si deve inoltre considerare la peculiarità degli indirizzi di studio presenti nel nostro Istituto e della possibilità che alcuni allievi “sfidino” le misure di protezione instaurate, anche solo allo scopo di “misurare” le proprie capacità tecniche.

3. Strategie di protezione

Le strategie di protezione delle tre reti messe in atto dall’Istituto prevedono:

- A. utilizzo di uno o più firewall per impedire l’accesso dall’esterno ai computer della scuola e per filtrare l’accesso dalla rete interna a quella esterna;
- B. uso di un sistema di autenticazione centralizzato mediante un dominio differente per ciascuna rete;
- C. utilizzo di un server per il controllo degli accessi alla rete;
- D. utilizzo regolamentato dell’accesso agli elaboratori e alla rete per gli allievi solo se accompagnati dal personale della scuola incaricato della vigilanza;
- E. mediante appositi software i docenti abilitano gli allievi all’utilizzo a tempo di Internet;
- F. un sistema di registrazione e monitoraggio delle attività di tutte le reti;
- G. tutti gli utenti devono cambiare la password personale ogni 90 giorni.

Tuttavia, a dispetto delle forme di prevenzione e controllo attuate dalla scuola, non è escluso che l'utente durante la navigazione possa imbattersi in materiale non appropriato e/o indesiderato.

È altresì possibile che gli utenti della rete, utilizzando in modo improprio le connessioni in rete e delle risorse tecniche della scuola, provochino danni quali violazione di diritti d'autore, violazione di sistemi protetti e altro.

L'Istituto Severi non può farsi carico delle responsabilità per il materiale non idoneo trovato o per eventuali conseguenze causate dall'accesso alla rete.

Per questi motivi gli utenti della rete, in particolar modo gli allievi, dovranno acquisire le strategie necessarie alla gestione corretta delle informazioni on-line attraverso:

- A. la verifica della correttezza, validità e attendibilità delle informazioni cui si accede;
- B. l'utilizzo di proposte comparate e alternative;
- C. rispetto dei diritti d'autore e dei diritti della proprietà intellettuale.

Dovranno inoltre essere pienamente coscienti degli eventuali rischi cui si espongono collegandosi alla rete e invitati a segnalare ai docenti eventuali siti di pornografia, violenza, razzismo e simili in cui dovessero imbattersi.

Inoltre è opportuno che i docenti discutano con gli allievi la policy della scuola e li sensibilizzino sui problemi che possono verificarsi utilizzando Internet, in modo da favorire un utilizzo consapevole ed "etico" della rete.

4. Accesso ai servizi della rete didattica

L'accesso ai servizi della rete didattica di Istituto (dominio e connettività Internet) è possibile solo tramite autenticazione con nome utente e password personale (nel seguito, account).

L'intestatario di un account è l'unico responsabile delle eventuali azioni illecite e/o di disturbo compiute, nonché di tutto il materiale e i mezzi utilizzati con tale account. I file di log vengono conservati (per un periodo non superiore ai 180 giorni) in un luogo protetto e potranno essere consegnati all'autorità giudiziaria per l'identificazione degli autori di eventuali illeciti.

È responsabilità dell'utente non divulgare la propria password e modificarla con cadenza periodica.

Gli account personali vengono forniti, previa sottoscrizione di un documento di assunzione di responsabilità, con le seguenti modalità:

- A. al personale della scuola che ne fa richiesta, con validità fino alla cessazione del rapporto di lavoro o fino alla revoca di una delle due parti;
- B. agli allievi ad inizio anno scolastico, con validità fino a fine anno scolastico (31 agosto);
- C. ai corsisti di corsi organizzati presso l'Istituto Severi, nel caso la frequenza al corso renda necessario l'uso delle risorse di rete, con validità pari alla durata del corso stesso.

Per convegni organizzati presso l'auditorium dell'Istituto i cui relatori abbiano l'esigenza di accesso alla rete Internet, è prevista la possibilità di utilizzare un account temporaneo.

Tale account deve essere richiesto, tramite compilazione di un modulo di assunzione di responsabilità, al personale tecnico incaricato con almeno 5 giorni di anticipo e ha durata limitata alla durata del convegno stesso.

5. Accesso alla rete Wi-Fi

L'accesso alla rete Wi-Fi avviene nei seguenti modi:

- A. Punto di accesso **WiFiSeveri_edu**. Mediante installazione nel proprio dispositivo personale (o in comodato d'uso) del docente o dell'allievo, di un certificato digitale nominativo. L'operazione di installazione del certificato viene svolta dal personale tecnico della scuola. Il certificato ha una validità massima di 3 anni, può essere revocato.
- B. Punto di accesso **WiFiSeveri_guest**. Viene comunicata una password a formatori esterni e/o utenti ospiti che devono collegarsi ad Internet. La password viene cambiata il primo giorno di ogni mese.
- C. Punto di accesso **WiFiSeveri_fcl**. Riservato al *Future classroom lab*. Viene comunicata una password a formatori esterni, utenti ospiti o corsisti che devono collegarsi ad Internet. La password viene cambiata il primo giorno di ogni mese.

L'intestatario del dispositivo è l'unico responsabile delle eventuali azioni illecite e/o di disturbo compiute, nonché di tutto il materiale e i mezzi utilizzati con tale dispositivo. I file di log vengono conservati (per un periodo non superiore ai 180 giorni) in un luogo protetto e potranno essere consegnati all'autorità giudiziaria per l'identificazione degli autori di eventuali illeciti.

6. Regolamento per l'utilizzo di laboratori didattici connessi alla rete didattica di Istituto

Durante l'utilizzo della rete didattica dell'Istituto e accedendo a Internet dalla stessa **vanno sempre rispettate tutte le disposizioni di legge**.

Inoltre si dovrà rispettare il seguente regolamento:

- A. l'accesso ai laboratori e/o alle postazioni di informatica non è permesso agli allievi in assenza di un docente responsabile;
- B. l'utilizzo dei servizi della rete è autorizzato solo per scopi didattici;
- C. è vietato danneggiare in qualunque modo l'attrezzatura utilizzata, in particolare è vietato compromettere il funzionamento della rete e degli apparati che la costituiscono con programmi non autorizzati;
- D. è vietato modificare in qualsiasi modo la configurazione fisica e logica della rete. In particolare:
 - i. è vietato modificare la configurazione TCP/IP degli elaboratori che si utilizzano;
 - ii. non è possibile collegare alla rete didattica computer personali;
- E. è vietato l'utilizzo di credenziali altrui di cui si è venuti casualmente o intenzionalmente a conoscenza;
- F. sono vietati comportamenti lesivi dei diritti di altri, quali:
 - i. archiviare, inserire, accedere, diffondere in rete dati personali (e in particolare: informazioni su gusti, opinioni politiche o religiose, fotografie) propri o di terze persone;
 - ii. violare la privacy di altri utenti, ad esempio intercettandone la posta elettronica o accedendo senza autorizzazione ai loro file;
 - iii. violare la sicurezza di archivi e/o computer della rete;
- G. In caso di manutenzioni ordinarie o straordinarie, guasti o altri problemi non è garantito il ripristino di tutte o parte delle funzionalità dei sistemi o degli account, né tantomeno il rapido intervento o il preavviso su base personale. Nessun danno diretto o indiretto sarà attribuibile alla perdita di dati o al mancato utilizzo dei servizi abitualmente disponibili. È

responsabilità dei singoli utenti il salvataggio del proprio lavoro mediante copia dei file importanti.

La violazione del presente regolamento comporterà la sospensione dell'accesso alla rete e/o alle risorse informatiche, ferme restando eventuali responsabilità civili e penali del trasgressore.